IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	**Criminal No. 1:09-CR-384-01**
v.	:	
JOSEPH W. NAGLE	:	**Judge Sylvia H. Rambo**

M E M O R A N D U M

Before the court is Defendant Joseph W. Nagle's motion to suppress all electronic evidence obtained from the computers and server seized from the premises of Schuylkill Products, Inc. ("SPI") and CDS Engineers, Inc. ("CDS") on October 10, 2007.[1] (Doc. 41.) Specifically, Defendant argues that the Government indiscriminately rummaged through more than a million computer files from the electronic evidence seized from SPI and CDS, that the warrants used to justify the seizure were unconstitutional general warrants, unconstitutionally over-broad, and were executed in an unreasonable manner.

The Government argues that Defendant does not have standing to challenge the search and seizure of the electronic evidence because he cannot demonstrate that he had a reasonable expectation of privacy in the content of SPI's and CDS's computers, and as such he cannot show that his Fourth Amendment rights were violated by the Government's actions. The court held a hearing on June 24, 2010. Upon consideration of the evidence, the court agrees with the Government. Defendant has failed to demonstrate that he has a personal, reasonable expectation of privacy in the contents of SPI's and CDS's computer systems, and has failed to

[1] This motion was originally filed on behalf of Defendant Joseph W. Nagle and co-defendant Ernest G. Fink, Jr. However, on July 30, 2010, Fink entered into a plea agreement with the Government. On August 16, 2010, at his change of plea hearing, Fink withdrew his motion to suppress.

demonstrate that his Fourth Amendment rights were violated. Accordingly, Defendant's motion to suppress will be denied.

I. Background

Because the court determines that Defendant has not demonstrated that he had a reasonable expectation of privacy in the property searched and seized, the court need not delve too deeply into the facts underlying the methods employed by the Government to conduct its search of the electronic information seized. This is true because even if the Government's warrant were a general warrant or unconstitutionally over-broad, and even if the Government's search methods amounted to a general indiscriminate rummaging of electronic evidence, conclusions which this court does not reach, it is immaterial to the prosecution of Defendant because all of this would have been done at the expense of SPI's and CDS's Fourth Amendment rights as opposed to the Fourth Amendment rights of the Defendant. Accordingly, the court provides the following information as background to provide context for its decision.

A. The Alleged Fraud

At some point in 2007, the Government began an investigation into whether SPI, CDS, Marikina Construction Corporation and Marikina Engineers and Construction Corporation (collectively "Marikina"), a small Connecticut-based certified disadvantaged business enterprise ("DBE"), were engaged in a DBE-fraud scheme. The alleged fraud spanned a period of fifteen years from 1993 through 2008. *See, e.g., United States v. Campbell*, 1:08-CR-07, slip op. at 3 (M.D. Pa. July 1, 2010). During this time, Marikina received 336 subcontracts worth approximately

$119.4 million, making it PennDOT's largest recipient of DBE-designated funds. *Id.* These subcontracts were awarded to Marikina by general contractors to whom PennDOT had awarded the prime contract to perform federally funded highway work in Pennsylvania, and they generally called for Marikina to "furnish and install" bridge beams. *Id.* Most of the bridge beams were manufactured by SPI, but some required Marikina to install non-SPI products. *Id.*

Applicable federal regulations allowed general contractors to count the entire DBE contract amount, including the costs of supplies and materials obtained by the DBE, even if the suppliers of the materials were non-DBE entities, toward the general contractor's DBE goal. *See* 49 C.F.R. § 26.55(a)(1). Thus, despite the fact that for any given contract the cost of materials may make up the majority of the contract amount, the entire contract amount could be credited towards the general contractor's DBE goal if the DBE performed a commercially useful function.

Here, the Government alleges that Marikina did not perform a commercially useful function in connection with any of the PennDOT DBE subcontracts, and in reality, the subcontracts were actually found, negotiated, coordinated, performed, managed, and supervised by SPI and CDS personnel. Furthermore, upon receiving payment from the general contractor, Marikina remitted all of the funds to SPI if an SPI beam was used. If a non-SPI beam was used, Marikina paid the third-party for the beam and then remitted the balance of the funds to SPI. SPI would then kick-back a fixed amount to Marikina. Thus, with every contract which listed Marikina as the DBE, all of the work and all of the money (except some of the materials and the Marikina fixed fee) would go to SPI and/or CDS. This scheme resulted in money that the Government intended to go to

legitimate DBEs performing commercially useful functions, instead being funneled through Marikina directly to non-DBEs.

B. The Structure of SPI and CDS/Layout of the Companies

SPI was started as a family owned company in 1950 by Defendant's grandfather who ran the business until his death in 1980. (Doc. 73, Suppression Hr'g Tr. 153, June 24, 2010.) From 1980 through 2004, the company was run by Defendant's father and Ernest G. Fink ("Fink"), a co-defendant and uncle by marriage to Defendant. (*Id.*) Upon his father's death in 2004, Defendant assumed control of his father's ownership share. (*Id.*) At the time of the search in October 2007, Defendant owned 50.1 percent of SPI and Fink owned 49.9 percent. (*Id.*) CDS was started in 1985 by Defendant's father, and after his death was absorbed as a wholly-owned subsidiary of SPI. (*Id.*)

At the time the search warrant was executed, Defendant was the President and CEO of both companies, and Fink was the Chairman and Chief Operating Officer of both companies. (*Id.* at 154.) Both companies employed family and friends of the Nagle and Fink families. (*Id.*) All told, the company employed 150 people at the time of the search; however, only 12-15 people worked in the SPI corporate office and 6-8 people worked in the CDS office. (*Id.* at 156-160; *see also,* Doc. 50-2, Exhibit A to Gov't Br. in Opp'n to Defs.' Motion to Suppress, Descriptive Mem., at 7 of 29.) Although he was the President and CEO, Defendant testified at the suppression hearing that he did not supervise any employees on a day-to-day basis. (Suppression Hr'g Tr. 173-74.)

The corporate offices of SPI and CDS are two separate converted residences with multiple floors that have office workers both in cubicles and offices

on all levels. (*Id.* at 34.) The SPI office had more than fifteen rooms covering an area of 2500 to 3000 square feet. Defendant's office was on the second floor; it had a door that could be locked, and was private from the remainder of the offices. (*Id.* at 156-57.) As a part of his job, Defendant used a laptop computer that was owned by SPI. (*Id.* at 158-59.) Defendant's laptop docked at a station on his desk and he connected each day to SPI's computer network. (*Id.*) In order to access his computer and the company's network, Defendant had to log in using a username and password. (*Id.* at 159.) CDS's offices were located in another converted residence that was slightly smaller than the SPI office space.

The companies shared one computer network. (*Id.* at 161.) The network was hosted by a server, and it was used to conduct all or most of the companies' business. The server housed, among other things, the companies' financial records, payroll records, pricing information, estimating standards, and technical data. (*Id.* at 162.) The server was partitioned into different drives, and certain users were restricted to certain areas on the server. (*Id.* at 162.) It is not clear from the record whether Defendant had access to the entire server, or only part of it; however, Defendant testified that the server required a password to access it and that the only person whom he was aware of who could access the server directly was the IT administrator. (*Id.* at 189.) He also testified that he was not aware of how the server worked, and that he did not have access to the server itself. (*Id.* at 181, 189.)

Each employee who had a computer also had a company e-mail address, which was used to conduct company business. (*Id.* at 162-63.) In addition to using company e-mail for sending such things as financial records, scheduling information,

product details, beam pricing and sales information, e-mail was also used for the company to seek and receive legal advice. (*Id.* at 163.)

At the suppression hearing, Defendant testified that he would spend approximately three-fourths of his day on his computer, which he used for both personal and business purposes. For instance, Defendant testified that he used the computer for communication with attorneys, banking, home refinancing, as well as communication with his wife and his friends. (*Id.* at 165.) At the time of the search, Defendant did not have another e-mail address and used his company e-mail for all of his personal e-mail. He also testified that he did not authorize anyone else to use his computer or his e-mail, and that the only other person at either of the companies who would have done so was the "IT administrator." (*Id.* at 165:21.) Defendant also testified that he never used anyone else's computer at either company. (*Id.* at 185.)

C. The Warrants

On October 9, 2007, FBI Special Agent Thomas Marakovits applied to Magistrate Judge J. Andrew Smyser for warrants to search the premises of SPI and CDS. The SPI warrant identified the premises to be searched as (a) SPI's corporate administrative offices, located in a two-story building with a detached garage; (b) SPI's transportation office, located in a one-story building; (c) SPI's human resources and payroll office, located above the SPI manufacturing plant; and (d) certain vehicles parked at or adjacent to the SPI manufacturing plant. (*See* Doc. 42-2, SPI Warrant and Aff. of Probable Cause ("SPI Warrant").) The CDS warrant identified the premise to be searched as (a) the administrative offices of CDS, which include a detached garage, and (b) certain vehicles parked at or adjacent to the office.

(*See* Doc. 42-3, CDS Warrant and Aff. of Probable Cause ("CDS Warrant").) Both warrants specifically authorized the seizure of the business records of Marikina, its predecessors and affiliated operating entities, SPI and CDS for the years 1999 through the date of the warrant. (*See* Attach. B to SPI Warrant and CDS Warrant.) The warrants listed fourteen categories of business records that could be seized, including "Computers and computer equipment." (*Id.*) After completing his review of the warrants, Magistrate Judge Smyser signed both of them.

D. Search of SPI and CDS

On October 10, 2007, Special Agent Marakovits led a team of agents in executing the SPI and CDS warrants. During the execution of the warrants, agents from the FBI's Computer Analysis and Response Team imaged eleven computers and one server onsite, and thereby obtained duplicate copies of each computer's data for later analysis. (Suppression Hr'g Tr. 39-41.) Because the imaging of the information on the computers and the server was successful, the agents did not remove any computers or computer equipment from the premises of SPI and CDS, and did not review any data from the computers or the computer images at the search premises.

The images of the eleven computers and one server came from numerous locations at SPI and CDS, including employee offices. None of the imaged computers were located in Defendant's office, which did not contain a computer at the time of the search. (*Id.* at 190.)

II. Discussion

A. Legal Standard

Defendant seeks to suppress all of the electronic evidence seized from SPI's and CDS's computers and its server on the basis that this information was seized pursuant to a general warrant, and, if not a general warrant, then an overly broad warrant, as well as because of the procedures used by the Government to cull through the information once it was in their possession. However, "[t]o invoke the Fourth Amendment's exclusionary rule, [Defendant] must demonstrate that *his own* Fourth Amendment rights were violated by the challenged search or seizure." *United States v. Stearn*, 597 F.3d 540, 551 (3d Cir. 2010) (quoting *Rakas v. Illinois*, 439 U.S. 128, 132-34 (1978)) (emphasis added). These rights are violated only if "the disputed search and seizure has infringed an interest of the defendant which the Fourth Amendment was designed to protect." *Rakas*, 439 U.S. at 140. "Significantly, a defendant's Fourth Amendment rights are not violated by the introduction of evidence obtained in violation of a third party's rights." *Stearn*, 597 F.3d at 551 (citing *Rakas*, 439 U.S. at 139).

The proponent of a motion to suppress "bears the burden of proving not only that the search . . . was illegal, but also that he had a legitimate expectation of privacy in [the place searched]." *Stearn*, 597 F.3d at 551 (citing *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980)) (omissions and alterations in original). Thus, in the context of the Fourth Amendment's exclusionary rule, the question of whether a defendant has "standing" to assert a violation of the Fourth Amendment is simply "shorthand for the determination of whether a litigant's Fourth Amendment rights have been implicated," as opposed to another's Fourth Amendment rights. *United States v. Mosely*, 454 F.3d 249, 253 n. 5 (3d Cir. 2006). Evidence from an illegal

search is suppressed "only [as to those] defendants who are able to satisfy *Rakas's* 'standing' prong." *Stearn*, 597 F.3d at 554.

B. Standing

Here, the Government argues that Defendant has not demonstrated that any of his Fourth Amendment rights were implicated by the seizure and subsequent search of SPI's and CDS's computers or its server. The court agrees.

1. Computers

The evidence presented at the suppression hearing makes it clear that during its search of the SPI and CDS premises, the Government imaged computers belonging to SPI/CDS from multiple locations throughout the 28-acre campus. (*See* Suppression Hr'g Tr. 80, 183.) Specifically, the computers imaged were located in the private work space of employees other than Defendant, and Defendant testified that he never used any other employee's computer. (*Id.* at 183.) Certainly, Defendant's reasonable expectation of privacy cannot be said to include these areas. *See, e.g., United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 54 (D. Conn. 2002) (CEO of company lacked standing to challenge search of company laptop computer used exclusively by another employee). Moreover, Defendant testified that his laptop was not at the office on the day of the search and was not imaged. (Suppression Hr'g Tr. 190.) Finally, Defendant testified that the company did not monitor what its employees did on their computers, it did not have a computer use policy, and he was unaware of what was on any of these machines. (*Id.* at 183, 185.) These facts unequivocally demonstrate that Defendant knew nothing—except in the most general sense that the computers were used for work—about what was stored on the computers seized or how they were used; thus, he had no *personal* expectation

of privacy in any of the information that was imaged by the Government. *See, e.g., Triumph Capital Group, Inc.*, 211 F.R.D. at 54 (CEO of company lacked standing to challenge search of company laptop computer used exclusively by another employee).

2. Server

The same is true for the SPI and CDS server. The evidence at the suppression hearing demonstrated that the server stored various types of electronic files and could be accessed by all of the employees with accounts on the companies' joint computer system. (Suppression Hr'g Tr. 162, 195, 206.) The server was partitioned into different drives, at least one of which was a public drive that was available to anyone who had access to the server. (*Id.* at 181, 206.) The other drives could only be accessed by certain employees in the various departments within SPI and CDS; however, there was scant evidence about who had access to which drives. The only specific testimony was by Fink, who testified that five employees, including himself and Defendant, had access to all of the drives on the server. (*Id.* at 192.) However, Defendant himself testified that he did not know how the server worked or what was stored on it, except in the most general sense. (*Id.* at 181.) While Defendant also testified that the server was private, and that the companies took security measures to make sure that no one from the outside would have access, (*id.* at 187-88), there was no testimony that Defendant took steps to ensure that his information or user folder remained inaccessible to others.

There was testimony at the suppression hearing that Defendant had a separate "folder" located on the server that he accessed, which presumably contained e-mails and other information, but this information came from FBI Forensic

Examiner D. Justin Price, not Defendant. (*See id.* at 85.) Defendant did not present this information and does not mention it in his brief, and it was not established that the folder was protected by a password or that it was restricted to use only by Defendant. (*See id.* at 89-91.) In fact, at the hearing, Defendant candidly admitted that he did not know how the server worked:

> Q: And on that network you mentioned that, I guess, there's one file that has your user file on there. Were you aware of that when you worked there?
>
> A: I don't know the nuts and bolts of exactly how the server worked.

(*Id.* at 181:6-10.)

Furthermore, while counsel for Defendant tried to elicit from the Government's witness whether or not Defendant's user folder was restricted, he was unsuccessful:

> Q: Were you able to determine, however, that [Defendant] had a section of the server that was designated for his information?
>
> A: That's correct, yes.
>
> Q: And was that section on the server segregated from other users of the computer system?
>
> A: I am not aware of that.
>
> Q: Were you able – well, let me ask you this question. Generally, are you able to analyze the server to determine whether certain users have access to different portions of the server?
>
> A: That's correct, yes.
>
> Q: Did you attempt to do such an analysis on the Schuylkill/CDS server?
>
> A: No, I did not.

Q: So you don't know one way or the other whether Mr. Nagle's section of the server was secured so that other people at CDS or Schuylkill Products would not have access to it?

A: I do not know that.

(*Id.* at 88:2-19; *see also id.* at 90:23-91:6.) Counsel did not follow up with his own witnesses to demonstrate that Defendant's user file was in fact restricted for his private use. Without this information, Defendant has not established a reasonable expectation of privacy in his user folder or the information that was stored on the server. At best, Defendant has demonstrated that there were steps that he *could* have taken to demonstrate an expectation of privacy in the content of the information stored in his user folder, but there was no evidence presented that Defendant actually took the steps necessary to do this.

Defendant, as the proponent of a motion to suppress, bears the burden of proving not only that the search was illegal, but also that he had a legitimate expectation of privacy in the place searched. *United States v. Stearn*, 597 F.3d 540, 551 (3d Cir. 2010). Taken as a whole, the evidence adduced at the hearing does not demonstrate that Defendant had a personal expectation of privacy in the contents of the server. The security measures taken by the companies to ensure the privacy of their business records are relevant only to the standing of the corporations themselves, not Defendant. *See United States v. SDI Futures Health, Inc.*, 568 F.3d 684, 698 (9th Cir. 2009) ("The security measures that [the corporation] took to ensure the privacy of its business records are relevant only to the standing of the corporation itself, not of its officers."). None of the evidence at the hearing established that Defendant had exclusive use of the contents of the server or that he had a *personal* expectation that its contents would remain private. While he may have had the

expectation that, as President and CEO of SPI and CDS, the contents of the companies' server would remain private, he had this expectation in his official capacity as an executive and officer of these corporations as opposed to himself as an individual. *See id.* at 696 ("[A]n employee of a corporation, whether worker or manager, does not, simply by virtue of his status as such, acquire Fourth Amendment standing with respect to company premises. . . . As always, a reasonable expectation of privacy does not arise *ex officio*, but must be established with respect to the person in question.").

3. Status as the Majority Shareholder of SPI and CDS

In his brief, Defendant asserts that his status as a majority co-owner of SPI and CDS gives him standing because both businesses were "family owned and operated." (*See* Doc. 76, Defs.' Supplemental Br. in Supp. of Mot. to Suppress at 23-25.) In support, Defendant references the Ninth Circuit's decision in *United States v. Gonzalez, Inc.*, 412 F.3d 1102, 1117 (9th Cir. 2005). A review of the facts of that case demonstrates how it is distinguishable from the facts of the present case.

In *Gonzalez*, the Ninth Circuit held that a father and son who owned "a small, family-run business housing only 25 employees at its peak" had standing to challenge a wiretap that had been installed at the business. *Id.* Among other things, the Ninth Circuit pointed out that the father and son had exercised managerial control over the day-to-day operations of the offices where the intercepted conversations occurred, and they also had exercised full access to the building. *Id.* at 1116-17. However, the ownership of SPI and CDS is dissimilar. First, CDS was a wholly owned subsidiary of SPI, and as of September 2008, SPI employed approximately 150 employees—or six times that of the business in *Gonzalez*—and operated on a

28-acre site throughout multiple buildings. (Suppression Hr'g Tr. 167; Doc. 50-2, Exhibit A to Gov't Br. in Opp'n to Defs.' Motion to Suppress, Descriptive Mem., at 7 of 29.) Furthermore, SPI had a ten-person management team, and Defendant supervised all SPI employees only "in an indirect way." (Suppression Hr'g Tr. at 174.) Thus, the court finds that *Gonzalez* is distinguishable, and believes that the facts presented here are, as the Government points out, more analogous to those confronted by the Ninth Circuit in *SDI Future Health, supra*, a case decided after *Gonzalez.*

In *SDI Futures Health*, the owners were controlling shareholders of a business whose headquarters was approximately a fifty person office. 568 F.3d at 697. Like Defendant, the SDI Futures Health owners worked in the office and "set its general policy as officers," however, they did not "personally manage[] the operation of the office on a daily basis." *Id.* The Ninth Circuit distinguished its earlier decision in *Gonzalez*, and held that the owners of SDI Futures Health had to show "some personal connection to the places searched and the materials seized" to challenge the search of workplace areas outside of their personal offices. *Id.* at 698. The court believes that Defendant must show the same, and that he has failed to do so.

None of the evidence presented at the hearing demonstrates that Defendant had a personal expectation of privacy in the content of the seized electronic information. Defendant's computer was not seized or imaged, and he failed to adduce sufficient evidence to allow the court to conclude that he had an expectation of privacy in the content of the electronic information stored on the server. As such, Defendant has not demonstrated that any of *his* Fourth Amendment

rights were violated, and thus his ownership of the companies whose records were seized is irrelevant. *See Stearn*, 597 F.3d at 551 ("[A] defendant's Fourth Amendment rights are not violated by the introduction of evidence obtained in violation of a third party's rights.")

IV. Conclusion

Because none of Defendant's Fourth Amendment rights were violated, there is no reason to reach a determination about the constitutionality of the Government's search methods. Doing so would be a futile waste of judicial resources. *See Stearn*, 597 F.3d at 554 (finding that evidence from an illegal search is suppressed only against defendants who are able to satisfy *Rakas's* "standing" prong). Accordingly, the court will deny Defendant's motion to suppress electronic evidence. An appropriate order will follow.

s/Sylvia H. Rambo
United States District Judge

Dated: September 1, 2010.

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	**Criminal No. 1:09-CR-384-01**
v.	:	
JOSEPH W. NAGLE	:	**Judge Sylvia H. Rambo**

O R D E R

In accordance with the accompanying memorandum of law, **IT IS HEREBY ORDERED THAT** Defendant's Motion to Suppress Electronic Evidence, (Doc. 41), is **DENIED.**

s/Sylvia H. Rambo
United States District Judge

Dated: September 1, 2010.